Captain Midnight, HBO, And World War III

Satellite Jamming For Fun, Profit, And Global Suicide

BY DONALD GOLDBERG
Illustration By Elwood H. Smith

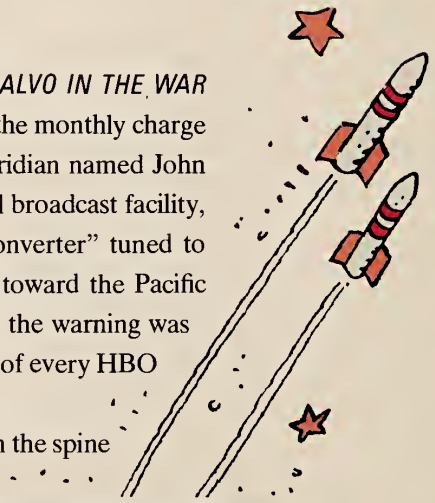
★ *SHORTLY AFTER MIDNIGHT ON APRIL 27, A BROADCAST TECHNICIAN AT THE HOME BOX OFFICE* facility in Hauppauge, Long Island, realized he had a problem. HBO viewers across the country knew it too: the network broadcast of *The Falcon and the Snowman* had disappeared, replaced by a message superimposed on a set of color bars: "Goodevening HBO. From Captain Midnight. $12.95/month? No way! (Showtime/Movie Channel beware!)"

The statement was a warning: backyard satellite dish owners would not pay the monthly charge instituted three months earlier to decode the now-scrambled Home Box Office programs they were used to getting free from the heavens.

The HBO technician realized that somebody else was using his company's satellite channel. He quickly grabbed a telephone and dialed the number for Hughes Communications, the satellite's owner. But Hughes officials on the night shift had no answers for HBO. They too were watching the message in amazement.

HBO's standard operating procedure when there's trouble with the broadcast calls for boosting the power. So, hoping to overcome this unknown intruder and get the movie back on the air, the technician turned up the knobs from the usual 125 watts of power. But Captain Midnight held fast. As the battle for control over the satellite channel wore on, HBO would eventually pump 2,000 watts' worth of broadcast signal to the satellite. Finally, fearing that a further escalation in wattage might damage the satellite, HBO surrendered.

Captain Midnight had won, and within four and a half minutes, he was gone.



★ *AT THE PUSH OF A BUTTON, CAPTAIN MIDNIGHT HAD FIRED THE FIRST SALVO IN THE WAR* against satellite scrambling in a way that went far beyond the immediate issue of the monthly charge for home dish owners. Nearly three months later, on July 22, a 25-year-old Floridian named John MacDougall turned himself in to federal authorities. Working from a commercial broadcast facility, MacDougall, as Captain Midnight, had patched his message through an "upconverter" tuned to HBO's frequency, sent it through an amplifier, and spun his transmit antenna toward the Pacific Ocean at a spot some 22,300 miles up. With the flick of a switch, at 12:32 A.M., the warning was beamed off of the Hughes Communications Galaxy I satellite and into the homes of every HBO viewer east of the Mississippi.

His brief message, that home satellite viewers would fight back, sent chills down the spine of every broadcast executive in the country. Captain Midnight had exposed the utter vulnerability of the entire satellite communications system to hackers, pranksters, or

worse. It was something that had been brought up from time to time but had never been taken seriously until now: the very ease with which the multi-billion-dollar industry could be disrupted, toyed with, and jammed.

"This person practiced video terrorism," said Stephan Schulte, Showtime vice president. "What he did was . . . tamper with the communications system of the United States of America. He opened up a can of worms."

It was video terrorism, all right, but Showtime and HBO are the least of the worries. Massive amounts of sensitive Defense Department information are carried along the same commercial satellite networks that MacDougall exposed as vulnerable to the acts of satellite saboteurs. This information, ranging from encrypted telephone calls to routine orders, is at the mercy of any Captain Midnight with more on his mind than satellite scrambling.

In fact, many of the Pentagon's own satellites have virtually no protection from jamming, whether by the Kremlin or by a lone technician. These communications channels carry some of the military's most vital information, including emergency action messages that tell the U.S. nuclear arsenal around the world that it's time to launch, that World War III has started and nuclear winter is about to begin.

The implications of Captain Midnight's exploits are enormous. Vital military messages, like the sending of nuclear "go-codes," are a cornerstone of nuclear deterrence, the certainty that the Pentagon can launch its weapons. If Captain Midnight had chosen to point his antenna at a Pentagon satellite instead of at HBO, the officers who monitor those channels might have assumed that the Soviet Union, about to fire its bombs at U.S. shores, was taking the first step by jamming the ability of the United States to retaliate.

And it's anybody's guess what the reaction of the Joint Chiefs of Staff might be in the time they would have to react—in the six or eight minutes it takes for a Soviet missile fired from a submarine off the East Coast of the United States to obliterate Washington.

★ *JUST HOW MUCH THE PENTAGON* has to lose at the hands of a Captain Midnight was revealed at a Capitol Hill hearing on a hot, sticky morning in June. Donald Latham, the assistant secretary of defense for command, control, communications, and intelligence, in charge of the workings of U.S. nuclear forces, made the following statement: the Pentagon spends more than a billion dollars a year to lease communications channels on commercial satellites, including Westar, Satcom, Comstar, and Anik. "A great deal of [the Defense Department's] industrial, administrative, and logistic business, especially within the continental United States, is transmitted over satellite channels," Latham said.

According to *Defense Electronics* magazine, the Pentagon leased 1,144 circuits—which equals roughly 10 percent of the total channels in orbit—from commercial satellites in 1982, the latest year for which figures are available.

"The other major satellite use is by defense contractors," Latham added. "And while the Department of Defense does not have control over these private enterprise decisions, we do have the right to demand security for our classified data and protection for our private information."

On The Satellite Trail

All sources for this article are publicly available and unclassified. One of the reports was obtained from confidential sources only after official requests for a complete copy were denied by the Federal Communications Commission. FCC officials informed the author that the National Security Agency had stepped in to block the release of the documents on national security grounds. The reports, however, are unclassified and are required by federal law to be made public upon request.

Other than to promise that future Defense Department satellites would have protection from the likes of Captain Midnight, Latham said little about the Pentagon's own satellites, which he described as carrying the military's "most important and critical circuits, those which support command and control of our force."

But in the meantime, the commercial satellite industry and many of the Pentagon's satellites are extremely susceptible to anyone with a smattering of know-how, money, and the urge to do damage. The necessary equipment—a sizable antenna, a signal generator, and a high-powered transmitter—is advertised in industry magazines. Lesser versions can be picked up on the surplus market, and an enterprising saboteur can manufacture his own jamming equipment.

Ironically, satellite saboteurs have a distinct advantage over other types of terrorists: it's difficult to get caught. Government and industry experts agree that the technology is not yet in place to pinpoint the location of a satellite hacker from his jamming signal alone. MacDougall, who was fined $5,000 and placed on a one-year probation, was caught because a vacationer had overheard a phone call. The characteristics of his video typewriter, known as a text generator, offered investigators further clues, and after being hunted for three months—often in the wrong places—MacDougall turned himself in. As it was, investigators had to survey 580 of the nearly 2,000 licensed U.S. facilities that MacDougall could have used.

★ *EVERY YEAR MORE AND MORE OF* America's business is conducted by satellite. Tens of thousands of long-distance phone calls are routed to the heavens and back. Television programs, banking transactions, billing services, electronic mail, weather information, oceanographic data, spy missions for the CIA, and infrared mapping—all use the dozens of U.S. satellites orbiting the earth.

Most communications satellites are in geosynchronous orbit, meaning that they orbit 22,300 miles over the equator at the same speed as the earth's rotation and thus appear to remain over one spot. Communications satellites are essentially relay stations located in space and are designed to receive a certain frequency, amplify that message, and send it almost instantaneously back to earth. On the ground, that signal is scooped up in a parabolic-shaped antenna, or dish, that may be located anywhere within the area the satellite covers, which is known as the "footprint." A geosynchronous satellite can cover as much as a third of the planet's surface, though typically the footprint is much smaller. The heavens are so crowded with geosynchronous satellites that they must be spaced at least two degrees apart to avoid interfering with one an-

other.

Captain Midnight just happened to pick transponder 23 on Galaxy I—located at 134 degrees west longitude and receiving signals beamed at a frequency of 6,385 megahertz (equal to 6,385 million cycles per second)—for his four-and-a-half-minute message. Transponders, or channels, on the orbiting satellites are programmed to respond to specific frequencies; each transponder on a satellite—most commercial versions have about 24—is programmed for a different frequency. That ensures that the various satellite channels don't block each other out.

But a transponder has no way of telling the difference between signals of the same frequency. Channel 23 on the Galaxy I satellite knows only that it is to relay signals sent at 6,385 megahertz, so when Captain Midnight beamed his defiant message skyward at that frequency with more wattage than HBO, he overpowered *The Falcon and the Snowman.*

Locating the exact positions of both commercial and military satellites, obviously the first step for Captain Midnight and for any who would follow in his footsteps, is no great feat. Commercial satellites must give that information to clients who lease the transponders; the clients, in turn, must distribute it to the various users, be they television affiliates or telephone companies. In any case, the information is readily available, since the Federal Communications Commission must assign and license the various satellite locations and frequencies. In addition, several books and guides provide the information (see sidebar, page 49). Armed with one of the satellite guides, the Captain could just as easily have aimed at AT&T's Telestar 301 satellite, positioned at 96 degrees west longitude. If he had, tuning his transmitter to 6,065 megahertz, he would have wiped out the CBS network feed to its affiliates.

Or he might have selected Satcom's F2R satellite by aiming his antenna at 72 degrees west longitude. Depending on which frequency he chose, he would have blocked Voice of America's foreign language broadcasts, television shows sent to U.S. troops in Central America by the American Forces Radio and Television Service, or any of 4,000 phone calls on circuits leased by MCI.

And if he were feeling particularly venturesome, Captain Midnight might have aimed at a spot at 100 degrees west longitude, above the Galápagos Islands, situated off the coast of Ecuador, and set his frequency at 293.975 megahertz. In that case, he would have jammed a channel on the U.S. Navy satellite Fleetsatcom 1, which is used to send emergency wartime messages from the president to U.S. submarines, silos, and bombers, telling them to launch their nuclear weapons.

Wide World

THE MIDNIGHT MANIFESTO THAT PUSHED THE FALCON AND THE SNOWMAN *OFF THE AIR.*

★ *JOHN PIKE OF THE FEDERATION OF* American Scientists, a renowned expert on military satellites, says "the Soviets have never jammed any of our satellites." That's because, according to Pike, Moscow wants neither to anger the Pentagon nor to give away its jamming capabilities. Pike says that some jamming may occur from time to time that appears accidental, but in general the Defense Department has little hands-on experience with its satellites being interfered with.

But according to a study done for AT&T in September 1980, the Iranians were able to jam U.S. communications during the aborted attempt to rescue the U.S. hostages in Iran earlier that year. That mission ended in disaster for the United States and President Jimmy Carter after a sandstorm downed two helicopters, and a helicopter and a tanker plane crashed, killing eight soldiers. The operation depended on precise coordination between U.S. troops stationed off Oman and Iran, and in Egypt, all ultimately taking orders from Washington.

"Communications were apparently monitored and jammed by both sides, so that there was an 'electronic battle' for several hours," reported the study, prepared for AT&T by SRI's Strategic Studies Center in Arlington, Virginia.

Imagine a solitary Iranian soldier, trained by Americans before the Shah's overthrow and now taking orders from his country's fundamentalist leaders. He may have been fighting sleep during the early morning hours of April 25 as he kept an eye on his monitors, watching for unusual electronic signals beamed across the country. Suddenly, a mass of unintelligible transmissions lit up the screens, jolting him awake as he tried to figure if the signals were counterrevolutionary propaganda or some sinister CIA plot.

His first reaction might have been to flip the switches that would send jamming pulses against these mysterious signals. And if the AT&T study is accurate, American electronics experts would have responded with all the muscle they had, jamming every Iranian radio signal in sight to keep its military from finding out about the raid.

Officially, there is no evidence that the mission was in any way compromised by electronic jamming, but in 1982 *Newsweek* reported that at least

—Continued on page 48

Captain Midnight

CONTINUED FROM PAGE 29

one communications breakdown had occurred. According to *Newsweek*, a key U.S. undercover agent who had infiltrated the Iranian capital of Tehran before the rescue attempt was late in getting word that the mission had been aborted, because his satellite communications link to Egypt was interrupted by "atmospheric conditions." The AT&T study, however, left wide open the possibility that Iran had jammed U.S. efforts: "Some common carrier channels were utilized, which means public/private cooperation in preparing the operation. . . . It may well also be that the cooperation was compromised by monitored communications."

★ *AS DONALD LATHAM PROMISED* at the June hearing, future military satellites will include state-of-the-art protection against the jamming, "exploiting," and "spoofing" of satellites. Captain Midnight "exploited" HBO's satellite channel by substituting his show for the regularly scheduled movie. He might just as easily have "spoofed" the satellite by sending false or confusing signals to its main control receiver, an act that could have disoriented or even ruined the satellite and cost Hughes Communications tens of millions of dollars to fix or replace it.

But despite Latham's bravado, the Pentagon's next generation of satellites, Milstar, won't be ready until the 1990s. And recent rocket disasters—including the space shuttle, the air force's Titan launches, and the European Ariane—have put satellites years behind schedule. In the meantime, according to experts from several federal agencies, there's no way to protect the fleet of civilian and military satellites now in use.

"Communications relays on air force satellites permit some channels to be used by anyone with the right kind of radios and antennas," said Major Robert Orlando of the air force Electronics System Division. On one occasion, Orlando said, air force technicians discovered a foreign country broadcasting music over an air force satellite channel.

George Knouse, a former Pentagon satellite analyst now at the Communications Division at NASA, said that with about $5,000 worth of equipment, NASA's experimental ATS-3 satellite, an older communications relay that will be replaced in several years, can be accessed and jammed.

"No one wants to recognize that we're very vulnerable, particularly since we're so dependent on satellites for communications," said Joseph Conte, the National Weather Service's manager for the Emergency Broadcast System. Conte has been fighting a proposal to use weather satellites as backup for the Emergency Broadcast System because they are so susceptible to jamming and to the weather itself.

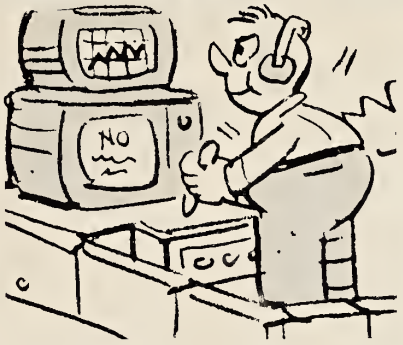
A recent article in the Washington, D.C.-based *Defense News* said that "if the Army went to war today, some officers predict U.S. electronic jamming will be about as effective on allied communications as it is on the enemy's."

And even state-of-the-art protection might not live up to its promise, because it's far easier to jam than to protect against jamming. The most secure method of keeping an outsider from jamming a vital communications channel is called "frequency hopping" and involves spreading the message across a large spectrum of frequencies, making the message difficult to jam unless you know the sequence. The technology, however, is too heavy and expensive for commercial satellites, is only in place in a handful of military satellites, and is not entirely foolproof. A study done for the Defense Communications Agency in 1983 looked at four possible antijam technologies, including one proposed by the National Security Agency, and concluded that "none of the [four] systems are jamproof."

★ *JOHN MACDOUGALL IS NOT THE* first "Captain Midnight"; the name has been used by phantom radio pirates for years. Bob Cooper, Jr., who publishes *Coop's Satellite Digest* and is generally considered the father of the home satellite industry, says the first electronic jammer to use the name appeared more than a decade ago, "a sort of 'electronic Zorro' riding about the countryside," breaking into radio broadcasts and leaving messages of "social significance." Since then, many citizens band radio enthusiasts and ham radio oper-

Home Jamming: A Do-It-Yourself Guide

★ *WHAT DOES IT TAKE TO BE A CAPTAIN MIDNIGHT?*



Any backyard electronics buff can go to a local parts outlet and put together a rudimentary jamming system, though it might not do more than put a few lines of static across the broadcast for a short time.

But John MacDougall's stunt, putting on his own show in place of HBO's, was more sophisticated than the relatively simple jamming of a commercial or military satellite transmission. It takes more power to replace someone else's signal altogether than it does to put static through that signal. Power, when it comes to satellite transmissions (or any radio signal for that matter), is a function of three ingredients: the output of the transmitter, the size of the antenna dish, and, to a lesser degree, location.

The backyard satellite dish industry, already in battle with the broadcasters who want to scramble their programs, was mortified by the bad publicity stemming from the Captain Midnight incident. Industry publications have taken great pains to show that no part-time mechanic using parts from his garage could duplicate MacDougall's feat.

But there are no laws governing who can buy electronic equipment as there are with nuclear materials or other weapons designed by the military. FCC regulations only apply when you turn the system on, and by then it's too late.

The first step is obtaining a transmitter. HBO officials say they normally send their signals at 125 watts and gave up their battle with Captain Midnight at 2,000 watts for fear of damaging the satellite. A transmitter eapable of putting out 2,000 watts, then, will generally defeat a commercial signal, though the commercial transmitter might have more power in reserve.

All that's really needed to put up some interference, according to Chris Schultheiss, former editor and publisher of *STV* magazine, is a 200-watt transmitter, built for the telephone company years ago and available in surplus stores or at ham radio conventions for under $500. A larger transmitter, putting out 1,000 watts, sells for about $30,000. One industry official said he was recently offered a 4,000-watt transmitter for $40,000, though a new one of that capacity would be much more expensive.

Three other minor pieces of equipment are needed for the transmission system. The first is a microwave signal generator, used for testing satellite-receiving equipment and costing about $2,000. The generator simply produces the microwave signal, which then must be turned to the right frequency, somewhere in the 6,000 megahertz range, by an upconverter. It also sells for about $2,000. Finally, a modulator, at a price of about $1,000, is needed to turn the frequency into a jamming "noise."

The other major piece of equipment is the dish; the larger the dish, the more damage that can be done. A backyard satellite dish, typically less than 4 meters in diameter, doesn't stand much of a chance against a 10-meter dish used by many commercial broadcasters. But a jammer with a 10-meter-diameter antenna is a little big to hide in the backyard, and the manufacturers are part of a tightly knit group; officials know who is buying equipment that large. Neither problem, however, is insurmountable.

A dedicated satellite saboteur isn't likely to care who knows how big a dish he has; presumably, his escape has already been planned. And if the dish is ordered for an island hideaway, like Cuba or any of the thousands of Caribbean isles within reach of most U.S. satellites, it will be beyond the long arm of U.S. law.

And it's not even necessary to draw attention to yourself by buying a dish. Industry experts say plenty of crafty hackers have built their own 10-meter dishes, which have been pulling satellite programming out of the sky for years. You can also use somebody else's dish: Perry Klein, a former president of the Radio Amateur Satellite Corporation—which operates its own ham satellites in orbit—points out that numerous seldom-used radio-astronomy dishes ranging in size from 10 to 30 meters are sprinkled across the countryside. A handful, Klein says, are in West Virginia, just a three-hour drive from Washington. If you were assembling a feed designed for the frequency, a transmitter and a generator could be plugged into one of these unused dishes.

If it's portability you're after, a half-million dollars will get you a mobile satellite transmitting station from one of any of a half-dozen companies, complete with a power supply, a transmitter, and a sizable dish. These stations are widely advertised in industry publications and are used, for example, by television networks broadcasting from remote locations.

Location is also a factor in the success of a jamming operation. All else being equal, whichever signal is closer to the center of the satellite's receiving footprint will have the advantage in jamming that satellite. A would-be Captain Midnight ean gain an early advantage by setting up as close to the center of his target's footprint as possible.

When it comes time to start jamming, any one of a number of publications will help you target your signals. For $197, you can buy *The 1986 Satellite Directory* from Phillips Publishing; those who want to save money can read it for free at the FCC's public reading room in Washington. It includes a description of each satellite with its location, frequencies, and services available.

For only $39.95, Florida-based expert Mark Long offers a more complete guide. Long's *World Satellite Almanac* gives a rundown of the frequency used for each transmission on every commercial satellite in the world, but does not include channels used by the Defense Department.

NASA itself distributes the industry standard, *The Satellite Situation Report*, available free from its operations supply branch in Greenbelt, Maryland. It gives an updated analysis, without locations or frequencies, of every identified satellite. *Aerospace Daily* publishes its own annual update of space launches and tends to be a little more accurate than NASA's report.

The government must by law distribute individual bulletins compiled by NORAD, the Pentagon office responsible for traeking space objects and incoming missiles. The bulletins include all the details needed to track an object from the ground.

The most detailed guide to military satellites has been compiled by Larry Van Horn and is available for $14.95 from Grove Enterprises in Brasstown, North Carolina. *Communications Satellites* gives the exact locations of a variety of the Pentagon's geosynchronous satellites and the frequencies used for each channel. Van Horn claims that all of his information was gathered from unclassified sources and from extensive monitoring of the satellites. However, some industry officials have accused him of publishing classified data. —*D.G.*

ators have adopted the pseudonym. Now the name, apparently taken from a World War II–era radio serial, is sure to be synonymous with video terrorism in the future.

And while MacDougall's act was not the first instance of satellite transmissions being interfered with, it appears to have been the first confirmed deliberate attack on a commercial satellite. Last October, channel 15 on Galaxy I—which receives signals at 6,225 megahertz and is used by superstation WOR-TV to send programs to affiliates—was blocked for 13 hours, though it may have been an accident, the kind of thing that happens when a programmer fires up the transmitter and flips through the channels.

The Disney Channel also experienced unexpected interference last October when one of its programs was interrupted for about 90 seconds by an X-rated show from the Fantasy Unrestricted Network, better known as "the Fun Channel." There is no evidence that the screwup was anything more than a high-tech accident, and the blue movie, a Disney spokesperson assured reporters, was too fuzzy to see any details.

And Alan Rockoff, a Middlesex County, New Jersey, prosecutor, caught seven teenagers last year accessing a computer link to a commercial satellite, enabling them to move control grids that pivot to handle overseas calls.

The Captain Midnight caper reads remarkably like a fictional piece that appeared in last November's issue of *STV* magazine, an industry publication based in Shelby, North Carolina. The article details the jamming of the HBO satellite by a mythical "Captain Kid," who held HBO hostage by jamming the transmission until the station stopped scrambling its signals.

With a 7-meter dish—somewhat smaller than HBO's 11 meters—and high-powered professional equipment, MacDougall had access to one of about 2,000 licensed commercial uplink facilities in the United States. But the $500,000 cost of such a setup is certainly not out of reach of a wealthy hacker or a video terrorist with some well-placed supporters in governments hostile to the United States.

And a cheaper version, according to Chris Schultheiss, could be built for less than $10,000. Schultheiss is the former editor and publisher of *STV*. A 4- or 5-meter antenna coupled to a 250-watt transmitter sending out electronic pulses at various frequencies could, according to Schultheiss, "put nasty lines across the picture." That type of equipment, while not capable of overpowering a military satellite, could easily make a television show unwatchable or a telephone call inaudible.

"Reporters, interviewing engineers and technicians for stories," recounted the *STV* piece about Captain Kid, "soon learned that the equipment necessary to generate such a high-powered pulse signal had been on the surplus electronics market for years, available for practically nothing. The equipment, outdated but perfectly usable radar transmitters, was originally produced by the thousands for the U.S. Army."

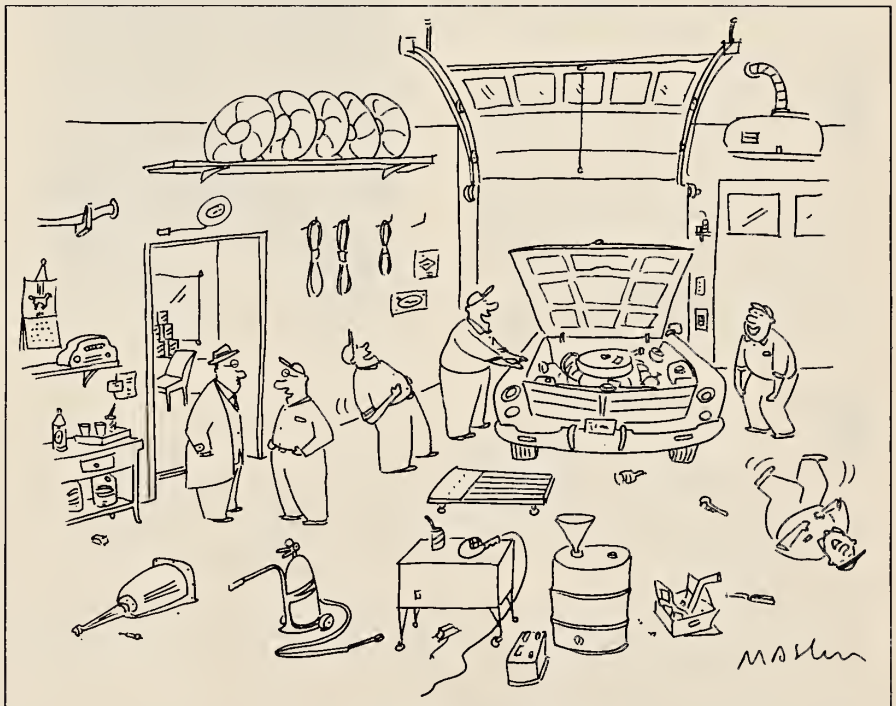
Charles Magin, an FCC official at the commission's Laurel, Maryland, facility, which is responsible for policing the airwaves, confirmed that surplus transmitters are available and added that much of what is available is more suited for military than civilian communications.

Other equipment, which sells for between $5,000 and $6,000 and sends out narrow microwave signals, is also on the market. Some of the equipment was built years ago for the telephone company; other types of transmitters were used by the old Civil Air Patrol.

★ *THE THREAT OF TERRORISM OR* sabotage to the satellite communications network was outlined at a closed meeting on January 29, 1985, in the tenth-floor conference room of AT&T's Washington office. There, a dozen members of the FCC's National Industry Advisory Committee met with officials from the National Security Agency, the Pentagon, and the FCC.

According to the publicly available minutes, John Boning, an RCA consultant and chairman of the advisory committee, opened the proceedings by detailing a briefing he had received two weeks earlier from the CIA, the FBI, and the Federal Emergency Management Agency. The topic: the terrorist threat to communications satellites.

The intelligence experts had divided the threat into three categories: "state-supported terrorists," "internal terrorists," and "crazies." No further details were given by Boning, but the Reagan administration generally defines state-supported terrorists as those with the resources of another country behind them. They take orders from governments hostile to the United States and, in the Reagan worldview, have both unlimited funds and expertise at their disposal.



"Your car's acting so funny we'd like to keep it another day."

The second category, internal terrorists, includes homegrown groups that operate primarily inside the United States, and would presumably have some military training and as much as a million dollars available for their activities.

The third category consists of the crazies, the backyard hackers who for one reason or another have gone off the deep end. A crazy, the thinking goes, would be intelligent though unpredictable, might have as much as $100,000 saved up, and would be upset enough about something to try to do some serious damage. John MacDougall would fall into this category by default, though the term *crazy* underestimates his abilities and intelligence.

At the closed meeting, Boning limited the discussion to those Reagan-age bogeymen in the first group. "The primary threat is from the state-supported terrorists who physically exist in this country," Boning reported. "They are organized, equipped, trained, and capable. Many of them are identified and are tracked by government agencies.

"Their modus operandi is never very clear. They're very clever, they use surprise to the maximum extent, and they desire spectacular results toward interrupting the status quo of orderly government. They capitalize on fear.

"The terrorist threat is real and can be anticipated when it is politically expedient for the terrorist to attack," Boning told the meeting.

Of course, neither Boning nor the other industry representatives there were so concerned that they were willing to spend the millions necessary to protect future satellites.

"The satellite carriers," Boning said, "must be very careful in protecting against these threats lest their costs escalate to the point that their business picture is so burdened by protective systems that they can no longer be competitive."

★ *PERHAPS THE MOST VULNERABLE* military satellite link is also one of the most vital. It is known in Pentagon parlance as Afsatcom and is considered by former Pentagon analyst Bruce Blair to be "the key satellite program designed specifically for strategic communications." Blair is the author of *Strategic Command and Control*, a Brookings Institute publication, and has also written extensively on the Defense Depart-

ment's control of its nuclear forces.

Last year Blair authored a highly classified report for the congressional Office of Technology Assessment on the gaping holes in the nuclear command structure. The Pentagon refused at first even to show members of Congress Blair's report.

Afsatcom, Blair says, is actually a number of transponders carried on board a variety of other satellites. The most important of those are attached to the four working Fleetsatcom satellites, including the one orbiting over the Galápagos Islands. Of the four satellites carrying the vital Afsatcom channels, two are in range of Cuban jammers and two are within reach of Soviet soil. The exact positions of the satellites were revealed and later published by a congressional committee in 1978.

"Afsatcom is . . . very vulnerable to jamming, a fact that has long been known and widely recognized," Blair argues. It's "fairly easy for a hacker to jam," he said. "The military would be caught off guard . . . [and] would have difficulty ascertaining they were being jammed, or what to do about it."

Then–Assistant Defense Secretary Gerald Dinneen admitted as much publicly at a 1979 hearing when he told Congress that current communications satellites, including Afsatcom, had very little if any antijamming capability and could be effectively "neutralized." Seven years later, the same satellites are still being used, and their antijamming capabilities have not changed.

It's impossible to say for sure what would happen if a satellite saboteur began jamming the Afsatcom channel. In times of low-level military alert, Bruce Blair contends, the Pentagon might not even realize it was being jammed.

But in times of rising tensions or concern over some international incident, the U.S. armed forces would be at a higher level of alert. In that case, the jamming of a military satellite would be taken very seriously.

"One of the 'least implausible' scenarios for the initiation of strategic nuclear war involves Soviet attack on U.S. satellites," states the September 1980 AT&T report, officially known as *Basic Telecommunications Issues Affecting U.S. National Security and Survival*. The satellites studied in the report remain aloft.

Picture, then, a future Captain Midnight alone at his isolated but well-stocked hideaway, somewhere in the Southwest within range of both the Fleetsatcom 1 satellite over the Galápagos Islands and perhaps the Fleetsatcom 4 satellite over the Marshall Islands. There, hidden in a clearing, is the Captain's homemade 11-meter dish, tied into his own commercially available transmitters, signal generators, and modulators—all the hardware needed to put together an effective jamming system.

Let's say the Pentagon is on high alert, perhaps because tensions have flared in the Persian Gulf, or perhaps just because the president is flexing his military muscles. U.S. Air Force officers are closely watching for any sign of irregular electronic activity—a jammer in Cuba, or maybe a Soviet ship off the Gulf of Mexico.

Captain Midnight decides to strike. Turning his antenna toward the sky, he slowly sends out a jamming pulse on an Afsatcom frequency, turning up the power and waiting for the fun to begin.

The military brass, unprepared for what's appearing on the monitors, panics. The first reaction is a quick flip through the channels to see if the other frequencies also are being jammed. Captain Midnight has planned well: he has sent up a pulse first on one frequency, then on a second, and so on until he has hit as many of the channels as possible—thus foiling any attempts to stop his jamming.

The military officers can't figure out exactly what's happening. They know only one thing: someone is attempting to block one of their most important satellites, the one needed if tensions get so hot that both Washington and Moscow would burn. From there it's easy to jump to the frightening conclusion—that the Soviets or their allies are making the first move in a nuclear war by trying to block the U.S. ability to launch its own bombs.

Of course, the Soviets are in the same boat; their satellites are easy to find and just as simple to jam. Captain Midnight might next turn his antenna toward a different spot in the sky and jam a Soviet satellite. And, having played both sides against the middle, Captain Midnight could just sit back and watch the fireworks.

Donald Goldberg is a senior reporter in Washington, D.C., for the syndicated Jack Anderson column.